



• PRAXISLEITFADEN · AUSGABE 2026

eIDAS 2.0: die **EUDI-Wallet**, was wir wissen, was wir nicht wissen

Alles Wissenswerte über die europäische digitale Identitäts-Wallet (EUDI-Wallet), um Ihre Prozesse schon heute vorzubereiten, ohne blind auf ein noch unsicheres System zu setzen.

🕒 10 Min. Lesezeit

📅 Wallets Ende 2026

👤 Banken · Telekommunikation · Retail

Die Verordnung **eIDAS 2.0**, in Kraft seit Mai 2024, setzt einen präzisen Zeitplan für die Einführung der **EUDI-Wallet**. Start Ende 2026, verpflichtende Integration für Banken und Telekommunikationsanbieter Ende Dezember 2027. Der Rahmen steht, doch viele konkrete Aspekte bleiben unklar und wirken sich direkt auf Ihre Business- und IT-Entscheidungen aus. Eines ist sicher: Richtig angegangen, ist diese Regulierung eine **Business-Chance**, weniger Friktion, weniger Betrug, mehr Konversion. Dieser Leitfaden zeigt zudem **die spezifische Dringlichkeit jeder Branche**, ob Bank, Telekommunikation oder Retail, mit konkreten Anwendungsfällen pro Geschäftsfeld.

1 Das Funktionsprinzip

DEFINITION

Die **EUDI-Wallet** ist eine digitale Identitäts-Wallet, die von jedem Mitgliedstaat bereitgestellt wird. Sie ermöglicht es europäischen Bürgern, ihre Identität nachzuweisen und bestimmte Dokumente an Dritte (Bank, Anbieter, Behörde) zu übermitteln, mit dem Vertrauensniveau „hoch“, gleichwertig mit einem physischen Ausweisdokument.

3 Schlüsseltermine zum Merken

Ende 2026

Start der Wallets

Bereitstellung

Ende Dez. 2027

Verpflichtende Integration

Banken & Telekommunikation

2030

Adoptionsziel

80% der EU-Bürger

Die User Journey in 4 Schritten



QR-Code scannen

Der Dienst zeigt einen QR-Code an, den der Nutzer mit seiner Wallet scannt



Authentifizierung

Biometrie oder PIN-Code zum Öffnen der Wallet



Einwilligung

Der Nutzer bestätigt, welche Daten mit dem Dritten geteilt werden



Übermittlung

Der Dienst erhält staatlich zertifizierte Daten: nichts abfotografieren, nichts erneut eintippen

Garantierter Mindestinhalt: die PID



Identitätsdaten

Name, Vorname, Geburtsdatum, Staatsangehörigkeit: die vom ausstellenden Staat zertifizierte Basisidentität



Vertrauensniveau „hoch“

Gleichwertig mit einem physischen Ausweisdokument: Die Wallet profitiert vom höchsten Vertrauensniveau



Ergänzende Dokumente

Adressnachweis, Gehaltsabrechnungen, Diplome... und perspektivisch die starke Authentifizierung von Zahlungen, wie in der Verordnung vorgesehen



Zum Merken: Ab Ende Dezember 2027 müssen Banken und Telekommunikationsanbieter die EUDI-Wallet als Identifizierungsmittel in ihren Onboarding-Prozessen akzeptieren.

Der Rahmen steht, doch **viele konkrete Aspekte bleiben unklar** und wirken sich direkt auf Ihre Business- und IT-Entscheidungen aus. Vier große Unsicherheitszonen prägen heute die Debatte.



#1 · Zeitplan der Attestierungen

Die PID (Identitätsdaten) wird Ende 2026 verfügbar sein. Für die **weiteren Dokumente** (Adresse, Gehalt, Diplome) wurde jedoch kein Zeitplan kommuniziert.

Eingeschränkte Planbarkeit



#2 · Tempo der nationalen Einführung

Italien ist in Produktion, Dänemark hat seine Wallet gestartet. Frankreich testet (France Identité ist noch nicht zertifiziert), Deutschland peilt Anfang 2027 an. **30 bis 50 Wallets erwartet**, noch nicht interoperabel.

Ungleiches Rollout-Tempo



#3 · Nationale Varianten

Die Durchführungsrechtsakte sind seit Dezember 2024 veröffentlicht. Doch jede nationale Implementierung behält **ihre eigenen Varianten**, und die tatsächliche Interoperabilität muss sich erst beweisen.

Interoperabilität unbewiesen



#4 · Tatsächliche Adoptionsrate

Die Nutzung ist bereits Realität: **über 100 Mio. Europäer** verfügen über eine nationale digitale Identität (80-95 % in den nordischen Ländern, 83 % in Italien). Bleibt eine **hybride Übergangsphase von 5 bis 10 Jahren**, in der Wallet und klassische Prozesse nebeneinander bestehen.

Hybrid 5–10 Jahre



Strategische Konsequenz: Angesichts dieser Unsicherheiten trägt nur eine Strategie: schon jetzt **flexible** Prozesse aufbauen, die die Wallet aufnehmen können, sobald sie da ist, ohne von ihr abhängig zu sein. Und das Garantieniveau der Wallet ist bereits heute erreichbar: das **NFC-Auslesen** des Chips im Ausweisdokument, staatlich signiert. Auf genau diesen Chip werden sich übrigens auch die Wallets stützen, um ihre Nutzer zu registrieren.

Selbst nach vollständiger Einführung wird die EUDI-Wallet nur **einen Teil des Bedarfs** abdecken. Fünf strukturelle Grenzen bleiben bestehen, nicht wegen mangelhafter Implementierung, sondern durch die Konzeption des Systems selbst.



#1 · Keine Finanzdaten

Die Wallet zertifiziert, **wer** der Kunde ist, nicht, **ob er zahlen kann**. Keine Einkünfte, keine Ausgaben, keine Bankhistorie.



#2 · Keine dynamische Betrugserkennung

Die Wallet zertifiziert die Identität zum **Zeitpunkt T**. Sie erkennt weder deepfakes noch synthetische Identitäten noch Strohänner.



#3 · Reine B2C-Lösung

Die Wallet deckt **kein KYB** ab: Wirtschaftlich Berechtigte, Bilanzen, Insolvenzverfahren müssen weiterhin anderweitig geprüft werden.



#4 · Auf Europa begrenzt

Die Wallet deckt **ausschließlich EU**-Bürger und in der EU ansässige Personen ab. Außerhalb der EU bleibt eine ergänzende Prüfung unverzichtbar.



#5 · Nur digitale Prozesse

Die Wallet ist für digitale Prozesse konzipiert. **Am physischen Point of Sale** ist sie ohne ergänzende Lösung nicht einsetzbar.

Die Wallet deckt 20 % des Bedarfs ab, nicht mehr

20 %

EUDI-Wallet
(zertifizierte Basisidentität)

80 %

Ergänzende Lösungen
(Bonität, Betrug, Geschäft, KYB)



Die Wallet allein genügt nicht. Bonität, Betrug nach dem Onboarding, Prozesse im Geschäft, AMLR-Konformität: alles Bereiche, die weiterhin in Ihrer Verantwortung liegen.

Über das Prinzip hinaus zeigen diese drei konkreten Situationen, was die EUDI-Wallet **nicht lösen wird**, selbst bei vollständiger Einführung.

1

Finanzierung im Autohaus

Ein Kunde möchte sein Fahrzeug direkt am Point of Sale finanzieren.

Problem:

Die Wallet funktioniert am physischen Point of Sale nicht. Zurück zum Papier: Fotokopie, manuelle Prüfung, 20 verlorene Minuten, null Garantie für die Echtheit.

2

Konto 3 Monate nach der Freigabe missbraucht

Ein Kunde wurde bei der Registrierung validiert. Drei Monate später tauchen verdächtige Transaktionen auf: Seine Zugangsdaten wurden kompromittiert, sein Konto wird von einem Betrüger genutzt.

Problem:

Die Wallet zertifiziert die Identität nur ein einziges Mal, bei der Registrierung. Danach? Kein Monitoring, keine Anomalieerkennung.

3

Kredit über 20.000 € mit versteckten Schulden

Ein Privatkunde beantragt einen Kredit über 20.000 €. Seine Identität wird mit der Wallet verifiziert. Sechs Monate später: Zahlungsausfall, 50.000 € nicht deklarerter Schulden kommen ans Licht.

Problem:

Die Wallet sagt,

wer

der Kunde ist, nicht,

ob er zahlen kann

. Zertifiziert ist die Identität, nicht die Bonität.



Ein gemeinsamer Nenner: In jedem dieser Fälle liefert die Wallet einen Baustein, die Identität, doch das Risiko liegt woanders. Neu gedacht werden muss die gesamte **Orchestrierung** des Prozesses.

Hinter dem Etikett „EUDI-Wallet“ verbergen sich **sehr unterschiedliche nationale Realitäten**. Der Umgang mit einer so simplen Angabe wie der Postadresse ist das anschaulichste Beispiel.

🕒 Frankreich · 2 Quellen, bis zu 1 Jahr Zeitverzug

- **Quelle 1: die Steuerverwaltung.**
Steueradresse, einmal jährlich aktualisiert (Mai-Juni).
- **Quelle 2: La Poste.** Postadresse, aktualisiert zum Zeitpunkt des Umzugs.
- **Bis zu einem Jahr Abweichung** zwischen den beiden Registern.

✓ Deutschland · zentrale Quelle, immer aktuell

- ✓ **Eine einzige zentrale Quelle.** Steueradresse = Postadresse.
- ✓ **Meldepflicht** für jede Adressänderung innerhalb von 3 Wochen.
- ✓ **Automatische Synchronisation** zwischen den Behörden.

⚠️ **Konsequenz:** Der „europäische Standard“ verbirgt sehr unterschiedliche nationale Implementierungen. Ihre Lösung muss **die Besonderheiten jedes Landes** beherrschen und mehrere Quellen aggregieren, um die Lücken zu schließen.

Der Betrug wartet nicht auf 2027: **+2.137 % deepfakes in drei Jahren, +300 % KI-generierte gefälschte Dokumente**. Sich auf eIDAS 2.0 vorzubereiten heißt also, das Garantieniveau jetzt anzuheben, **ohne ausschließlich** auf ein System zu setzen, dessen genauer Inhalt und dessen Adoptionsrate ungewiss bleiben. Gefragt ist eine Lösung, die Wallet UND klassische Prozesse **intelligent orchestriert**.



1 · Nicht alles auf die Wallet setzen

Die Wallet wird ein Identitätskanal unter mehreren sein, nie der einzige. Investieren Sie in eine Lösung, die alle Quellen je nach Verfügbarkeit orchestrieren kann.



2 · Nationale Besonderheiten antizipieren

Jedes Land hat seine Eigenheiten (z. B. Adresse in Frankreich vs. Deutschland). Ihre Lösung muss mehrere Quellen aggregieren können, um Lücken zu schließen und Unterschiede zu handhaben.



3 · In Orchestrierung denken, nicht in Integration

Eine automatische Logik: Wallet verfügbar? Nutzen. Ausweis mit Chip? NFC-Auslesen, seit Juni 2025 für die Privatwirtschaft geöffnet (Verordnung 2025/1208): das Garantieniveau der Wallet, schon heute. Sonst? Dokumentenbasierter Prozess. Ausländischer Kunde? Internationale Lösungen. Geschäftskunde? KYB.



4 · AMLR-Konformität sicherstellen

Die Wallet erleichtert die Basis-Identitätsprüfung, entbindet aber nicht von den Pflichten: CDD, EDD, Sanktions- / PEP-Screening, kontinuierliches Monitoring. Und um sie zu akzeptieren, ist eine Eintragung im Register der vertrauenden Beteiligten erforderlich (Verordnung 2025/848).



AMLR-Hinweis: Die von der Wallet zertifizierte Identität befreit nicht von den geldwäscherechtlichen Sorgfaltspflichten. CDD, EDD, Sanktions- / PEP-Screening und kontinuierliches Monitoring bleiben unverzichtbar.

Der regulatorische Zeitplan von eIDAS 2.0 gilt nicht für alle Geschäftsfelder gleichermaßen. Manche Branchen haben eine **terminierte gesetzliche Pflicht**, andere einen **akuten operativen Schmerzpunkt**, den die Wallet nicht lösen wird, wieder andere bleiben außerhalb des Pflichtbereichs, stehen aber vor derselben strukturellen Grenze: **Die Wallet funktioniert nur online.**



Banken & Fintechs

Terminierte gesetzliche Pflicht: verpflichtende Integration der EUDI-Wallet **Ende Dezember 2027** (Artikel 5f der Verordnung eIDAS 2.0, im Zusammenspiel mit der AMLR, anwendbar ab dem 10. Juli 2027, für das Onboarding auf Distanz).

Die Frage lautet nicht mehr „ob“, sondern „wie orchestrieren“: die Wallet akzeptieren, wenn der Kunde sie hat, einen klassischen Prozess vorhalten, wenn nicht, ohne Bruch in der Geldwäsche-Compliance. **Die ersten Wallet-Ausschreibungen zirkulieren bereits** in der Branche.

Pflicht Ende Dez. 2027



Telekommunikation & große Rechnungssteller

Dieselbe verpflichtende Frist 2027, und ein deutlich akuterer Schmerzpunkt: Die **Aktivierung von SIM-Karten im Geschäft** erfordert schon heute eine physische Identitätsprüfung, die die Wallet, konzipiert für Online-Prozesse, nicht abdeckt.

Solange die Wallet den physischen Point of Sale nicht bedient, bleibt die Identitätsprüfung im Geschäft ein regulatorischer und operativer blinder Fleck, der schon heute zu schließen ist. Genau dort entscheidet sich der Betrug beim Vertragsabschluss.

Akuter Schmerzpunkt: SIM im Geschäft



Retail, Auto & Point of Sale

Keine gesetzliche Pflicht analog zu Banken und Telekommunikation, aber dieselbe strukturelle Grenze: Die Wallet funktioniert **nur online**. Im Autohaus oder im Geschäft, ohne Anbindung an die Wallet, bedeutet das die schlichte Rückkehr zum Papier.

Der physische Point of Sale bleibt noch lange ein Prozess, der unabhängig vom eIDAS-Zeitplan abzusichern ist: Finanzierung im Autohaus, Schlüsselübergabe, Abholung im Geschäft. Die Prüfung am Point of Sale ist schon heute ein täglicher Bedarf der Branche.

Keine gesetzliche Pflicht, täglicher Anwendungsfall



Fazit: Ob gesetzliche Pflicht oder nicht, jede Branche hat ihren eigenen Grund, nicht bis zur Frist 2027 zu warten: ein regulatorischer Zeitplan, ein bereits vorhandener operativer Schmerzpunkt oder eine strukturelle Grenze der Wallet, die nicht verschwinden wird.



Der Meelo-Ansatz: Anpassung an Ihre Prozesse

Die Wallet löst 20 % des Problems (die zertifizierte Basisidentität). Meelo löst die **restlichen 80 %**: Bonität, Betrug, KYB, AMLR-Konformität, Prozesse im Geschäft. Eine einzige Integration, und **Meelo passt sich Ihren Prozessen an, nicht umgekehrt**: online, im Geschäft oder in der Filiale, in Frankreich wie international.

Wallet allein vs. Meelo

WALLET ALLEIN

Zertifizierte Identität, mehr nicht

Die EUDI-Wallet liefert einen wesentlichen Baustein: den Nachweis, wer der Kunde ist, mit dem Vertrauensniveau „hoch“.

Deckt nicht ab: Finanzdaten

Deckt nicht ab: Betrug nach dem Onboarding

Deckt nicht ab: KYB (Briefkastenfirmen)

Deckt nicht ab: Kunden außerhalb der EU

Deckt nicht ab: Prozesse im Geschäft

MEELO

Intelligente Orchestrierung, End-to-End

Meelo orchestriert die EUDI-Wallet **und** die klassischen Prozesse und ergänzt alles, was die Wallet nicht abdeckt.

Identität: Wallet, NFC-Auslesen oder dokumentenbasiert

Bonität: Open Banking + Analyse der Nachweise

Betrug: KI und kontinuierliches Monitoring

KYB: Analyse von Unternehmen & Geschäftsführung

Konformität: AMLR + Prozesse im Geschäft

Die Abdeckung auf einen Blick

20 %

EUDI-Wallet
Basisidentität

80 %

Meelo
Bonität · Betrug · KYB · Geschäft

100 %

Des Bedarfs
abgedeckt

Was Meelo über die Wallet hinaus leistet



Bonität

Open Banking + automatische Analyse der Nachweise zur Bewertung der Rückzahlungsfähigkeit



Betrug

KI-Erkennung und kontinuierliches Monitoring, weit über die reine Momentaufnahme hinaus



KYB

Analyse von Unternehmen + Geschäftsführung: wirtschaftlich Berechtigte, Bilanzen, Insolvenzverfahren



Nationale Abdeckung

Aggregation nationaler Quellen, um die Besonderheiten jedes Landes abzudecken



Prozesse im Geschäft

Identitätsprüfung am physischen Point of Sale, genau dort, wo die Wallet nicht funktioniert



AMLR-Konformität

CDD, EDD, Sanktions- / PEP-Screening und kontinuierliches Monitoring integriert



Eine einzige Integration: Meelo orchestriert automatisch die EUDI-Wallet und die klassischen Prozesse und ergänzt, was die Wallet nicht abdeckt: Bonität, verhaltensbasierte Betrugserkennung, fortgeschrittenes KYB, AMLR-Konformität und Identitätsprüfung im Geschäft.